



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

HA

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/837,981	04/19/2001	Lee Ming Cheng	P-370.207	1407
7590	06/06/2005		EXAMINER	
JACKSON WALKER L.L.P. 112 E. Pecan Street, Suite 2100 San Antonio, TX 78205			TRUONG, THANHNGA B	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 06/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/837,981	CHENG ET AL.
	Examiner Thanhnga B. Truong	Art Unit 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 2/8/2005 (Amendment).
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1,2,5,7-10 and 12-14 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1,2,5,7-10 and 12-14 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
 5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____

[Signature]

[Signature]

DETAILED ACTION

1. Applicant's amendment filed on February 8, 2005 has been entered. Claims 1-14 are pending. Claims 3, 4, 6 and 11 are cancelled by the applicant and claims 1, 2, 5, and 7-10 are also amended by the applicant.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-2, 12, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dijakovic (US 6,351,539 B1), further in view of Ozluturk (US 6,148,053), and further in view of Vobach (US 5,307,412 B1) and Degele (US 5,297,207), and

a. Referring to claim 1:

i. Dijakovic teaches:

(1) A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) including random number generator and stream cipher generator comprising: a crypto-engine operable as either a random number generator or a stream cipher generator, and a controller (e.g., switch) for controlling the crypto-engine to operate either as the random number generator or the stream cipher generator, including three multiplexers controlled by the controller to supply signals selectively to and receive signals from the crypto-engine, in which a first multiplexer is arranged to receive a random number generator seed signal or a stream cipher generator key signal, a second multiplexer is arranged to receive dynamic synchronization signal and a constant synchronization signals, and a third multiplexer is arranged to receive an output signal from the crypto-engine and provide a random number output signal or a stream cipher output, respectively in each case [i.e., referring to Figure 2, Djakovic's invention is an encryption device which has a

random number generator and three block cipher mechanisms. The first block cipher mechanism takes a plaintext input and produces a first enciphered output based on the plaintext and on a first key. An exclusive-or mechanism takes as input the first enciphered output from the first block cipher and the output of the random number generator and produces a combined output. The second block cipher mechanism takes as input the output of the exclusive-or mechanism and produces a second enciphered output based on the output of the exclusive-or mechanism and on a second key. The third block cipher mechanism takes as input the output of the random number generator and produces a third enciphered output based on the output of the random number generator and on a third key. The first and second block cipher mechanisms differ from each other, with one preferably being the IDEA block cipher, and the other preferably being the Blowfish block cipher (column 2, lines 19-36)].

ii. However, Djakovic is silent about a controller (e.g., switch) for controlling the crypto-engine to operate either as the random number generator or the stream cipher generator. On the other hand, Ozluturk teaches:

(1) Referring to Figure 1 or Figure 5, the switch 14 connects the spread spectrum transmitter 10 with an input for either digital voice data or digital data (column 2, lines 48-50 of Ozluturk).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) combine the teaching of Ozluturk's switch into Djakovic's system for more flexibility in choosing between the two different generators.

iv. The ordinary skilled person would have been motivated to:

(1) combine the teaching of Ozluturk's switch into Djakovic's system for improving the security of block ciphers using cipher concatenation in combination with a random number generator. (column 1, lines 7-9 of Djakovic).

v. The combination of Djakovic/Ozluturk do not explicitly shows:

(1) a random number generator seed signal and a synchronization signals

vi. Whereas, Vobach and Degele teach:

(1) A pseudo-random number generator is a deterministic machine which, when initialized by a "seed" number, produces a string of digits which appears to be random (by passing various statistical tests). The output of a pseudo-random number generator is periodic, but the period can be made very long. When sender and receiver use pseudo-random number generators to produce the second, key, or encrypting sequence, they start with a common initializing "seed" and synchronize the outputs of their generators (column 1, lines 43-52 of Vobach). Degele teaches the invention deals with combinations of, and combinatorial processes performed on, the bits of a "seed" cryptographic key in order to produce a new, often larger and permissively much, much larger, cryptographic key, or "keystream", that is typically as, or more, cryptographically secure than is the "seed" cryptographic key itself. The combinatorial processes are typically recursive, and may typically be used to produce cryptographic keystreams of any desired length. The typically long output cryptographic key, or keystream, is usefully used to encrypt plain text, or to decrypt cipher text, data by any number of conventional cryptographic processes, including by a one time pad (**column 8, lines 20-32 of Degele**).

vii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) mention the use of a seed signal and synchronization signals (in Djakovic as modified) to provide a cryptographically secure keystream by an "amorphous" process (**Degele's abstract**).

viii. The ordinary skilled person would have been motivated to:

(1) mention the use of seed signals and synchronization signals (in Djakovic as modified) since the amorphous processes, should the one in use at any particular instance not be known to a code breaker, present a great practical difficulty to a cryptoanalyst in discerning either (i) the "seed" key, or (ii) the amorphous process(es) operating thereon, from the output keystream. Of course, the output

keystream is intended to be secret, and unavailable to the cryptoanalyst who typically has only cipher text data (**column 8, lines 36-43 of Degele**).

b. Referring to claim 2:

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

c. Referring to claim 12:

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

d. Referring to claim 13:

i. Dijakovic further teaches:

(1) a decision box for selecting whether the dual function generator is operating as a random number generator or a stream cipher generator and an attractor mapping table connected to the decision box for providing encrypted/decrypted data when the dual function generator is operating as a stream cipher generator [**i.e., referring to Figures 2 and 3, even though block ciphers may use the same key for encryption and decryption, they generally have different encrypting and decrypting modes. The various block ciphers used herein are in their respective encrypting modes when encrypting and in their respective decrypting modes when decrypting (column 3, lines 62-67)**].

3. Claims 5, 7-10, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dijakovic (US 6,351,539 B1), further in view of Ozluturk (US 6,148,053), further in view of Vobach (US 5,307,412 B1) and Degele (US 5,297,207), and further in view of Smith (US 5,216,750).

a. Referring to claim 5:

i. Dijakovic, Ozluturk, Vobach, and Degele teach the claimed subject matter except for:

(1) including the clipped Hopfield Neural Network pairs.

ii. However, Smith teaches:

(1) Computation system and method using hamming distance which include Hopfield neural networks in Figure 2 (**column 1, line 37 through column 2, line 22**).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include Hopfield neural networks (in Djakovic as modified) to preserve some sense of closeness in the known neural networks (**column 2, lines 57-62 of Smith**).

iv. The ordinary skilled person would have been motivated to:

(1) include Hopfield neural networks (in Djakovic as modified) to preserve closeness for encoding sensor output to neural network compatible input while retaining a large capacity to avoid data compression or resolution loss (**column 3, lines 11-14 of Smith**).

b. Referring to claims 7-10, 14:

i. These claims have limitations that is similar to those of claim 5, thus they are rejected with the same rationale applied against claim 5 above.

Response to Argument

4. Applicant's arguments filed February 8, 2005 have been fully considered and the new ground(s) of rejection is addressed above.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

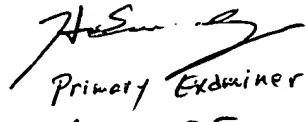
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date

of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.


Primary Examiner
AU 2135

TBT

May 29, 2005